

IN THE CLAIMS:

Please amend the claims as follows.

1. (Currently Amended) A method of recording transmitted digital data in which transmitted digital information is encrypted by a recording encryption key (E (NE)) and stored by a recording means on a recording support medium and ~~characterised~~ characterized in that an equivalent of the recording encryption key (E (NE)) is encrypted by a recording transport key (RT (A)) and stored on the support medium together with the encrypted information.

2. (Original) A method as claimed in claim 1 in which the information encrypted by the recording encryption key (E (NE)) comprises control word information (CW) usable to descramble a scrambled data transmission also recorded on the support medium.

3. (Previously Presented) A method as claimed in claim 1 in which the recording encryption key (E (NE)) and/or recording transport key (RT (A)) are stored on a portable security module associated with the recording means.

4. (Previously Presented) A method as claimed in any preceding claim 1 in which the transmitted information is encrypted prior to transmission and received by a decoder means before being communicated to the recording means.

5. (Previously Presented) A method as claimed in claim 4 in which the decoder is associated with a portable security module used to store transmission access control keys

(KO(NS), KO'(Op1, NS) etc.) used to decrypt the transmitted encrypted information.

6. (Original) A method as claimed in claim 5 in which the recording encryption key (E (NE)) and/or recording transport key (RT (A)) function in accordance with a first encryption algorithm (DES) and the transmission access control keys (KO(NS), KO' (Op1, NS) etc.) function in accordance with a second encryption algorithm (CA).

51
7. (Currently Amended) A method as claimed in claim 1 which the recording transport key (RT (A)) is generated at a central recording ~~authorisation~~ authorization unit and a copy of this key communicated to the recording means.

8. (Previously Presented) A method as claimed in claim 7 in which the recording transport key (RT (A)) is preferably encrypted by a further encryption key (KO(NSIM)) prior to being communicated to the recording means.

9. (Previously Presented) A method as claimed in claim 1 in which a central access control system communicates transmission access control keys (KO (NS), KO'(Op1, NS) etc.) to the recording means.

10. (Previously Presented) A method as claimed in claim 9 in which the transmission access control keys (KO(NS), KO' (Op1, NS) etc.) are communicated to a portable security module associated with the recording means.

11. (Previously Presented) A method as claimed in claim 9 in which the recording means directly descrambles transmitted information using the transmission access keys (KO (NS), KO'(Op1, NS) etc.) prior to re-encryption of the information by the recording encryption key (E (NE)) and storage on the support medium.

b1
12. (Previously Presented) A method as claimed in claim 9 in which the central access control system preferably encrypts the broadcast access control keys (KO(NS), KO' (Op1, NS) etc.) by a further encryption key (KO (NSIM)) prior to their communication to the recording means.


13. (Currently Amended) A method as claimed in claim 9 in which the recording means sends a request to the central access control system including information identifying the broadcast access keys needed (KO(NS), KO'(Op1, NS) etc.), the request of being-authenticated authentication by the recording means using a key (KO(NSIM)) unique to that recording means.

14. (Previously Presented) A method as claimed in claim 1 using a decoder means and associated security module and a recording means and associated security module and in which a copy of the recording transport key (RT (A)) is stored in the security module associated with the decoder means and/or the security module associated with the recording means.

15. (Previously Presented) A method as claimed in claim 14 in which the recording

transport key (RT (A)) is generated by either the recording security module or decoder security module and communicated to the other security module.

16. (Original) A method as claimed in claim 15 in which the recording transport key (RT (A)) is preferably encrypted before communication to the other security module and decrypted by a key unique (KO(NS)) to that other security module.

 17. (Currently Amended) A method as claimed in claim 16 in which the decoder security module and recording security module carry out a mutual ~~authorisation~~ authorization process, the unique decryption key (KO (NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual ~~authorisation~~ authorization.

18. (Currently Amended) A method as claimed in claim 17 in which the mutual ~~authorisation~~ authorization step is carried out using, inter alia, an audience key K1 (C) known to both security modules.

19. (Previously Presented) A method as claimed in claim 14 in which the decoder security module possesses transmission access control keys (KO(NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form and a session key (K3 (NSIM)) re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key

(RT (A)).

20. (Previously Presented) A method as claimed in claim 19 in which the session key (K3 (NSIM)) is generated by the decoder security module or recording means security module and communicated to the other module in encrypted form using an encryption key (KO (NS)) uniquely decryptable by other security module.

21. (Previously Presented) A decoder means adapted for use in a method as claimed in claim 14 including a security module adapted to store a copy of the recording transport key (RT (A)).

22. (Previously Presented) A decoder means as claimed in claim 23 including a security module adapted to descramble transmitted information using one or more transmission access keys (KO(NS), KO' (Op, NS) etc.) prior to reencryption by a session key (K3 (NSIM)) for subsequent communication to a recording means.

23. (Previously Presented) A portable security module adapted for use in the decoder means of claim 23 and comprising at least a copy of the recording transport key (RT (A)).

24. (Currently Amended) A recording means adapted for use in a method as claimed in claim 1 comprising a security module for encrypting transmitted digital information by a recording encryption key (E (NE)) for storage on a recording support medium and ~~characterised~~ characterized in that the security module is further adapted to encrypt the

recording encryption key (E (NE)) by a recording transport key (RT (A)) for storage on the support medium.

25. (Currently Amended) A portable security module adapted for use in the recording means of claim 21 and ~~characterised~~ characterized in comprising a recording encryption key (E (NE)) for encryption of transmitted digital information for subsequent ~~reecordal~~ recording and a recording transport key (RT (A)) for encryption of the recording encryption key for subsequent ~~reecordal~~ recording.

26.-29. (Cancelled)